KONICA MINOLTA

All Covered

IT SERVICES FROM KONICA MINOLTA

USE **CASE**

ALL COVERED'S MANAGED COMPLIANCE SERVICES PREPARES A LARGE DENTAL PRACTICE FOR OCR AUDIT

BACKGROUND: A multi-site dental organization was unprepared and facing an OCR (Office for Civil Rights) audit with possible fines for accidentally exposing over 4,000 ePHI records to public search engines. The breach was caused by an improperly configured computer server that was owned by the dental company and had not been updated for several months. The server was not properly connected to the private and secure network.

The organization also lacked documented procedures and processes for assessing and monitoring all its administrative tasks, physical facility security, information security systems, equipment, and applications connected with ePHI patient data. It also did not have appropriate check and balances or information security systems in place for authorizing access to patient databases and termination access to the patient databases.

SOLUTION: Through All Covered's Managed Compliance Services, we were able to assist the dental organization with a thorough HIPAA risk assessment to analysis the administrative, physical and technical safeguards that were currently in place. Then All Covered implemented a compliance portal to manage ongoing vulnerability scans for internal private and external public sites, maintain policies and procedures with audit logs and a single dashboard to show the current status of compliancy. After the HIPAA risk assessment, the dental practice could document all of their organization's assets whether it was in the wired or wireless network. Ongoing vulnerability assessments were planned out to safeguard the organization against any future breaches resulting from software upgrades before the software was deployed to the network. We helped write up their technology policies and procedures to authenticate users accessing their ePHI data as well as setting up user rights by role. Remediated the gaps found in the technical vulnerability assessment. Added a system to alert and notify key stakeholders of policies and procedures that needed review. Maintenance of vendor list and BAA agreement renewals. Ability to perform HIPAA compliance audit on vendors.

CURRENT COMPLIANCE STATUS: The organization has a better understanding and awareness of their HIPAA and compliance requirements. With the help of All Covered, they have implemented the necessary policies and procedures, and a compliance portal to review security risks and alerts in a timely manner. Employees have been trained on the organization's new policies and procedures and continue to grow their security and HIPAA knowledge-base with company-provided training.

Item #: ACHCCCompliance 09/2018-L

THE COST OF HIPAA NON-COMPLIANCE

Since HIPAA, which was signed into law in 1996, ever since the HIPAA Enforcement Act was passed, organizations that fail to implement the appropriate controls to protect healthcare data and the privacy of patients have been fined by the OCR. From 2011 to 2017, fines ranging from $2.5 million to $32.5 million have been issued for HIPAA violations. Not to mention the civil action lawsuits that can also be filed against an agency and providers for data breached on the ground of negligence.

Multi-million dollar monetary penalties have been issued for non-compliance, but a HIPAA-violation fine is one of the smaller costs that healthcare organizations and its vendors have to cover. Healthcare Organizations and its vendors experiencing even relatively small data breaches can see the cost of a data healthcare data breach spiral.

Without a dedicated HIPAA team, you might not know how far you are from closing the HIPAA gap. Even with a dedicated HIPAA team, organizations usually require additional outside consulting services to help them meet HIPAA requirements.